



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/593,026	05/14/2007	Stephen Wilson	58430/M1090	5711
23363	7590	09/16/2010	EXAMINER	
CHRISTIE, PARKER & HALE, LLP PO BOX 7068 PASADENA, CA 91109-7068				VAUGHAN, MICHAEL R
ART UNIT		PAPER NUMBER		
2431				
NOTIFICATION DATE			DELIVERY MODE	
09/16/2010			ELECTRONIC	

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

[pto@cph.com](mailto:pto@cph.com)

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>
	10/593,026	WILSON, STEPHEN
	<b>Examiner</b>	<b>Art Unit</b>
	MICHAEL R. VAUGHAN	2431

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 13 July 2010.  
 2a) This action is **FINAL**.                    2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 96-115 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) 96-115 is/are allowed.  
 6) Claim(s) \_\_\_\_\_ is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)          | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ .                                    |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____.   | 6) <input type="checkbox"/> Other: _____ .                        |

## **DETAILED ACTION**

The instant application having Application No. 10/593,026 is presented for examination by the examiner. Claims 96-98, 100-105, 113, and 114 are amended. Claims 96-115 are pending.

### ***Response to Amendment***

#### ***Claim Objections***

Claim objections are overcome by amendment.

### ***Response to Arguments***

Applicant's arguments filed 7/13/10 have been fully considered but they are not persuasive. Applicant alleges that the cited prior art, Wheeler, fails to show each and every claimed feature. Examiner respectfully disagrees.

In response to applicant's arguments, the recitation "anonymously indexing an electronic record system" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

In response to Wheeler not teaching "storing an asymmetric cryptographic private key under the control of a portable storage device of a registered user", this limitation is broader than argued. The claim does not require the storing of the private key into the portable storage device. In fact, the claim puts no limitation on where the private key is stored. Even if one assumes it is stored in the portable device, the claim does not require the device to already have been registered to the user at the time the key is stored. As such, Wheeler teaches a private key stored in the portable device which is then registered to a user (0107, 0137).

In response to Wheeler not teaching "storing an anonymous public key certificate, the anonymous public key certificate being associated with an asymmetric cryptographic public key matching the asymmetric cryptographic private key", the definition of 'anonymous' is brought into question. Examiner has given the word anonymous its broadest and most reasonable definition in light of the specification. Applicant's specification in paragraph 0072 of the PG-PUB, defines an anonymous public key certificate as a public key certificate that does not contain the name of the person to whom it is linked/issued. Wheeler's public and private keys are interpreted as anonymous and meeting this definition because they are purposely not identifying to the user. The keys are tied to the device but do not identify a user. Because the device is linked to the user and when messages are signed using the device's private key, the user is assumed to have authorized the message. However to a third party receiving the message they have no idea who signed the message. The specification does not provide for any special or novel way in which the keys are made anonymous. Therefore

the ordinary meaning is used to determine the scope of the claimed invention. With respect to the certificate, public key certificate contain public key. Again, the claim does not define where this certificate is stored. Wheeler teaches a device has a public and private key. The private key is securely retained within the device (0107). A public key certificate contains a public key signed or attested by a trusted party. If the certificate is anonymous it only contains the public key, not information to whom the key belongs. As such Wheeler teaches the public key of the device is signed by a trusted party, Secure Entity, thus creating a security certificate (0112). This certificate meets the requirements of an anonymous public key certificate because it contains the public key and does not identity the user of the public key. Therefore, Wheeler is found to teach the same anonymous system as claimed. Keys are used anonymously but are verified by a secure database. The keys are indexed to the device and the device is registered to a user with an account.

In response to Wheeler not teaching providing the portable storage device with information for associating the registered user with the portable storage device, Wheeler teaches a user inputs a PIN into the device to authenticate it (0138). Once authentication is complete, customer-specific information is associated with the public/private keys of the device through a linked database (0140).

In response to Wheeler not teaching “indexing within an electronic record system personal information of the registered user, whereby association of the information with the registered user is anonymously verifiable by use of the anonymous public key certificate”, paragraphs 0140-0141 address this feature. When a device is associated

with a user there is an index which points to a user's account (0141). The association of the personal information of the user is always verifiable through use of the private key. In other words, when the anonymous private key is used to sign a message, the public key which relates to the private key can be linked to the account through the secure database. An outside party or third party would have no knowledge of who used the device but the transaction could be traced to an account as discussed by Wheeler's wire transfer example (0157).

In view of the foregoing, Examiner must maintain the rejection in view of Wheeler. The claims are not distinguishable from the system of Wheeler.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 96-115 are rejected under 35 U.S.C. 102(e) as being anticipated by USP Application Publication 2003/0101344 to Wheeler et al., hereinafter Wheeler.

As per claim 96, Wheeler teaches a method for anonymously indexing an electronic record system, the method comprising:

storing an asymmetric cryptographic private key under the control of a portable storage device of a registered user (0107);

storing an anonymous public key certificate [security certificate is digitally signed by a trusted party to authentication the device's public key; 112], the anonymous public key certificate being associated with an asymmetric cryptographic public key matching the asymmetric cryptographic private key [0112, 0122 shows the certificate is linked to the public key which is in turn linked to the private key (0107); 0156 shows that the keys are certificate are all created anonymously and are tied to a device, not a user];

providing the portable storage device with information [PIN] for associating the registered user with the portable storage device (0102 and 0138); and

indexing within an electronic record system personal information of the registered user (0140), whereby association of the information with the registered user is anonymously verifiable by use of the anonymous public key certificate [anonymously verified because a digital signature is formed by anonymous private key attributed to a device for which there is a database linking the device to the user; 0142, 0156].

As per claim 103, Wheeler teaches an anonymously indexed electronic record system comprising:

a portable storage device for a registered user (0107), an asymmetric cryptographic private key being under the control of the portable storage device (0112),

the portable storage device being provided with information for associating the registered user with the portable storage device (0107);

a stored anonymous public key certificate [security certificate; 0165] associated with an asymmetric cryptographic public key matching the asymmetric cryptographic private key (0112),

an electronic storage indexing personal information of the registered user (0140, 0155), whereby association of the information with the registered user is anonymously verifiable by use of the anonymous public key certificate [anonymously verified because a digital signature is formed by anonymous private key attributed to a device for which there is a database linking the device to the user; 0156].

As per claims 97 and 104, Wheeler teaches the information for associating the registered user with the portable storage device is at least one of: human readable information; and machine readable information (0102).

As per claims 98 and 105, Wheeler teaches the portable storage device is at least one of: a smartcard; and an electronic passport (0100).

As per claims 99 and 106, Wheeler teaches the indexing comprises associating with each item of personal information of the registered user an electronic record pointer, and wherein the anonymous public key certificate contains the electronic record pointer (0165; the public key is linked to a secure database).

As per claim 100, Wheeler teaches storing of the asymmetric cryptographic private key under the control of the portable storage device comprises at least one of:

storing the asymmetric cryptographic private key in the portable storage device (0107); storing an access code in the portable storage device allowing access to the asymmetric cryptographic private key; and copying the asymmetric cryptographic private key into the possession of an authorized user (0102).

As per claims 101 and 107, Wheeler teaches digital signature codes are created for given data items within the electronic record system in order to explicitly link each digitally signed data item to the value of an electronic record pointer associated with the digital signature codes [the digital signature is intrinsically linked to the public key and therefore the associated database and its records; 0156].

As per claims 102 and 108, Wheeler teaches digital signature codes are created for given data items in the electronic record system using an asymmetric cryptographic private key issued to the registered person, where each digital signature code is interpreted as explicitly recording the consent of the registered person to the creation of each respective digitally signed data item [the digital signature is intrinsically linked to the public key and therefore the associated database and its records; 0156].

As per claim 109, Wheeler teaches the anonymous public key certificate [security certificate; 0165] contains a personal data component [security profile; 0017].

As per claim 110, Wheeler teaches the personal data component comprises biometric data of the registered user (0102).

As per claim 111, Wheeler teaches the asymmetric cryptographic private key is stored in the portable storage device (0107).

As per claim 112, Wheeler teaches an access code is stored in the portable storage device allowing access to the asymmetric cryptographic private key (0102).

As per claim 113, Wheeler teaches the asymmetric cryptographic private key can be copied with the registered user's authorization into the possession of an authorized user (0102).

As per claim 114, Wheeler teaches the authorized user is a health care professional authorized by the registered user to enter an update to the registered user's indexed personal information (0132 and 0136).

As per claim 115, Wheeler teaches a portable storage device for a registered user of an anonymously indexed electronic record system (0017), the portable storage device being provided with information [PIN] for associating the registered user with the portable storage device (0017, 0138), wherein an asymmetric cryptographic private key is under the control of the portable storage device (0107), wherein an anonymous public key certificate [security certificate] is associated with an asymmetric cryptographic public key matching the asymmetric cryptographic private key (0121, 0165), and wherein association of anonymously indexed personal information with the user is anonymously verifiable by use of the anonymous public key certificate [anonymously verified because a digital signature is formed by anonymous private key attributed to a device for which there is a database linking the device to the user; 0156].

***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR.

Art Unit: 2431

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431